WHAT IS CLAIMED IS:

1. A method for policing communications packets, comprising:

classifying the data stream into at least one traffic flow;

classifying at least one of the traffic flows into a plurality of first level subflows;

measuring a rate of each of the first level subflows associated with the traffic flow when the traffic flow reaches a predetermined bandwidth threshold; and

marking the packets associated with each of the first level subflows with one of a plurality of conformance indicators based on the measured rate of the respective first level subflow.

2. The method of Claim 1, further comprising:

assigning a rate limit to each of the first level subflows; and

comparing each first level subflow to its corresponding rate limit.

3. The method of Claim 2, wherein marking the packets comprises marking the packets based on whether the measured rate of each first level subflow exceeds its respective rate limit.

4. The method of Claim 1, further comprising classifying at least one of the first level subflows into a plurality of second level subflows.

5. The method of Claim 1, further comprising classifying at least one of the first level subflows into further levels of subflows to an n^{th} level of subflows.

6. The method of Claim 5, further comprising:

assigning a rate limit to each of the n^{th} level subflows; and

comparing each n^{th} level subflow to its corresponding rate limit.

7. The method of Claim 5, wherein marking the packets comprises marking the packets based on whether the measured rate of the respective n^{th} level subflow exceeds its respective rate limit.

8. The method of Claim 5, further comprising:

measuring a rate of each of the nth level subflows associated with its parent subflow; and

marking the packets associated with each of the nth level subflows with one of a plurality of conformance indicators based on the measured rate of the respective nth level subflow.

9. The method of Claim 1, further comprising monitoring each of the traffic flows to determine whether each respective traffic flow has reached the predetermined bandwidth threshold.

10. The method of Claim 9, wherein monitoring each of the traffic flows comprises monitoring for a triggering token level in a credit-token metering methodology.

11. The method of Claim 1, further comprising assigning a priority level to each of the first level subflows, wherein at least two of the priority levels are different so that at least one of the first level subflows has priority over another of the first level subflows.

12. The method of Claim 11, wherein the priority levels are effected by associating a rate limit with each of the subflows, and wherein marking the packets based on the measured rate comprises marking the packets based on whether the rate limit is exceeded for the corresponding subflow.

13. The method of Claim 1, further comprising adding a flow ID corresponding to the classified flow to a local header, and identifying a traffic flow to meter based on the flow ID.

14. The method of Claim 1, further comprising adding a subflow ID corresponding to the classified subflow to a local header, and identifying the first level subflow in which its rate is to be measured based on the subflow ID.

15. The method of Claim 1, wherein classifying the data stream into at least one traffic flow comprises classifying the data stream based on protocol layer information.

16. The method of Claim 15, wherein classifying the data stream based on protocol layer information comprises classifying the data stream based on layer-3 information.

17. The method of Claim 16, wherein classifying the data stream based on layer-3 information comprises classifying the data stream based on at least one of a source address and a destination address.

18. The method of Claim 1, wherein classifying at least one of the traffic flows into a plurality of first level subflows comprises classifying the traffic flow based on protocol layer information.

19. The method of Claim 18, wherein classifying the traffic flow based on protocol layer information comprises classifying the traffic flow based on layer-4 information.

20. The method of Claim 19, wherein classifying the traffic flow based on layer-4 information comprises classifying the traffic flow based on at least a port number.

21. The method of Claim 1, wherein classifying the data stream and classifying at least one of the traffic flows into a plurality of first level subflows comprises classifying the data stream and traffic flows based on any predetermined one or more fields in any embedded header of each packet.

22. The method of Claim 1, wherein measuring a rate of each of the first level subflows comprises metering each of the first level subflows using a credit-token methodology.

23. The method of Claim 1, wherein measuring a rate of each of the first level subflows comprises metering each of the first level subflows using a color-based methodology.

24. The method of Claim 1, wherein measuring a rate of each of the first level subflows comprises metering each of the first level subflows using an F-GCRA methodology.

25. The method of Claim 1, further comprising discarding packets of a non-conforming subflow which are marked with a conformance indicator indicating that the corresponding packets of the non-conforming subflow should be discarded.

26. The method of Claim 25, further comprising forwarding packets of a conforming subflow which are marked with a conformance indicator indicating that the corresponding packets of the conforming subflow should not be discarded.

27. The method of Claim 1, further comprising assigning a rate limit to each of the first level subflows, and wherein marking the packets comprises marking the packets associated with a subflow as non-conforming where the rate of the subflow exceeds its respective rate limit.

28. The method of Claim 1, further comprising assigning a rate limit to each of the first level subflows, and wherein marking the packets comprises marking the packets associated with a subflow as conforming where the rate of the subflow exceeds its respective rate limit but remains within the predetermined bandwidth threshold of the traffic flow.

29. The method of Claim 1, further comprising assigning a rate limit to each of the first level subflows, and wherein marking the packets comprises:

marking the packets associated with a subflow as conforming where the rate of the subflow exceeds its respective rate limit but remains within the predetermined bandwidth threshold of the traffic flow; and marking the packets associated with the subflow as non-conforming where the rate of the subflow exceeds both its respective rate limit and the predetermined bandwidth threshold of the traffic flow.

30. The method of Claim 1, further comprising allocating substantially all of the available bandwidth of the traffic flow to one of the subflows where the traffic flow has reached the predetermined bandwidth threshold and the other subflows are not utilizing bandwidth.

31. The method of Claim 30, wherein marking the packets comprises:

marking the packets associated with the one subflow as conforming where the rate of the subflow exceeds its respective rate limit but remains within the predetermined bandwidth threshold of the traffic flow; and

marking the packets associated with the subflow as non-conforming where the rate of the subflow exceeds both its respective rate limit and the predetermined bandwidth threshold of the traffic flow.

32. The method of Claim 1, further comprising assigning a rate limit to each of the first level subflows and allocating the available bandwidth of the traffic flow to a plurality of the subflows if the traffic flow has reached the predetermined bandwidth threshold, wherein the available bandwidth of the traffic flow is allocated to the plurality of subflows based on their respective rate limits and demand for bandwidth.

33. A method for providing layered policing of packets of a data stream, comprising:

parsing the data stream into a plurality of flows;

for any of the flows, identifying at least one characteristic common to a first subset of the flow;

associating a first drop probability with each of the packets of the first subset having the common characteristic, and associating a second drop probability to at least one other subset of the flow, thereby providing different drop probabilities for different subsets of the flow.

34. The method of Claim 33, wherein the first drop probability indicates that the packets of the first subset are to be dropped.

35. The method of Claim 34, wherein the second drop probability indicates that the packets of the at least one other subset are not to be dropped.

36. The method of Claim 33, wherein the first drop probability indicates that the packets of the first subset have a greater likelihood of being dropped prior to the at least one other subset of the flow.

37. The method of Claim 33, wherein parsing the data stream comprises respectively grouping the packets having predetermined common characteristics into the flows.

38. The method of Claim 37, wherein grouping the packets having predetermined common characteristics comprises grouping those packets having predetermined information in one or more header fields embedded in the packet.

39. The method of Claim 38, wherein the one or more header fields comprise header fields of a network layer header.

40. The method of Claim 39, wherein the header fields of the network layer header comprises at least one of a source address and a destination address.

41. The method of Claim 33, wherein identifying at least one characteristic common to the first subset of the flow comprises identifying common information in one or more header fields embedded in the packets to distinguish the first subset from the other subsets of the flow.

42. The method of Claim 41, wherein the one or more header fields comprise header fields of a transport layer header.

43. The method of Claim 42, wherein the header fields of the transport layer header comprises a port number.

44. The method of Claim 33:

further comprising identifying at least one characteristic common to a second subset of the flow; and

wherein associating a second drop probability to at least one other subset of the flow comprises associating the second drop probability with each of the packets of the second subset of the flow.

45. The method of Claim 44, wherein the first and second drop probabilities are equivalent.

46. The method of Claim 44, wherein the first and second drop probabilities are different.

47. The method of Claim 44:

further comprising identifying at least one characteristic common to an nth subset of the flow; and

wherein associating a second drop probability to at least one other subset of the flow comprises associating the second drop probability with each of the packets of the nth subset of the flow.

48. The method of Claim 33, wherein one of the subsets of the flow comprises all packets otherwise not associated with a subset defined by having common characteristics.

49. A packet policing system for providing layered policing of packets of a data stream, comprising:

A) a classifier to receive and parse the data stream into a plurality of traffic flows, and to parse at least one of the traffic flows into a plurality of subflows; and

B) a policing engine coupled to the classifier to receive each of the subflows, and to individually meter each of the subflows associated with each traffic flow in accordance with predefined subflow priorities assigned to each of the subflows.

50. The packet policing system as in Claim 49, wherein the policing engine includes a memory to store the predefined subflow priorities assigned to each of the subflows.

51. The packet policing system as in Claim 50, wherein the predefined subflow priorities include predefined rate limits.

52. The packet policing system as in Claim 51, wherein the policing engine includes a processor coupled to receive the rate limits for each of the subflows, to compare a subflow packet rate for each of the subflows to its respective rate limit, and to provide a conformance rating in response thereto.

53. The packet policing system as in Claim 52, further comprising an editing module coupled to the policing engine to modify each of the packets of each subflow with the conformance rating provided by the processor.

54. The packet policing system as in Claim 53, further comprising a packet drop module coupled to receive the modified packets from the editing module, and to accept or discard each of the modified packets based on the conformance rating.

55. The packet policing system as in Claim 49, further comprising a packet drop module coupled to receive the modified packets from the policing engine in response to the individual metering of the subflows.

56. A packet policing system for providing layered policing of packets of a data stream, comprising:

means for classifying the data stream into at least one traffic flow;

means for classifying at least one of the traffic flows into a plurality of first level subflows;

means for measuring the packet rate of each of the first level subflows associated with the traffic flow when the traffic flow reaches a predetermined bandwidth threshold; and

means for marking the packets associated with each of the first level subflows with one of a plurality of conformance indicators based on the measured packet rate of the respective first level subflow.

57. A packet policing apparatus for providing layered policing of packets of a data stream, comprising:

means for parsing the data stream into a plurality of flows;

for any of the flows, means for identifying at least one characteristic common to a first subset of the flow;

means for associating a first drop probability with each of the packets of the first subset having the common characteristic, and means for associating a second drop probability to at least one other subset of the flow, thereby providing different drop probabilities for different subsets of the flow.

58. A computer-readable medium having computer-executable instructions for policing communications packets, the computer-executable instructions performing steps comprising:

classifying the data stream into at least one traffic flow;

classifying at least one of the traffic flows into a plurality of first level subflows;

measuring a rate of each of the first level subflows associated with the traffic flow when the traffic flow reaches a predetermined bandwidth threshold; and marking the packets associated with each of the first level subflows with one of a plurality of conformance indicators based on the measured rate of the respective first level subflow.

59. A method for providing layered policing of packets of a data stream, comprising:

parsing the data stream into one or more flows;

parsing at least one of the flows into a high-priority subflow and at least one standard subflow;

enabling the high-priority and standard subflows to be monitored for bandwidth conformance when the flow reaches a predetermined bandwidth threshold;

marking the high-priority subflow as conforming while allowing the standard subflows to be marked as non-conforming if the flow becomes non-conforming;

where the flow has become non-conforming, adjusting the bandwidth of the standard subflows to bring the flow into conformance.

60. A method for maximizing exploitation of a contracted bandwidth for a flow, comprising:

parsing the flow into a high-priority subflow and at least one standard subflow;

assigning rate limits to the high-priority subflow and the at least one standard subflow;

monitoring packet conformance on a subflow level when the flow decreases to a predetermined bandwidth capacity;

providing guaranteed bandwidth to the high-priority subflow while providing best effort bandwidth to the at least one standard subflow, regardless of whether the flow has exceeded its contracted bandwidth;

if the flow has exceeded its contracted bandwidth, adjusting the bandwidth of the at least one standard subflow to bring the flow into conformance, while maintaining the guaranteed bandwidth to the high-priority subflow.